(2)

STUDY PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

ULTRA: A CASE STUDY

BY

MR. RAYMOND E. MILLER
United States State Department

DISTRIBUTION STATEMENT A: Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1991

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

Unclassified
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION
Unclassified

1b. RESTRICTIVE MARKINGS

2a. SECURITY CLASSIFICATION AUTHORITY

2b. DECLASSIFICATION / DOWNGRADING SCHEDULE

3. DISTRIBUTION / AVAILABILITY OF REPORT
Approved for public release.
Distribution is unlimited.

4. PERFORMING ORGANIZATION REPORT NUMBER(S)

5. MONITORING ORGANIZATION REPORT NUMBER(S)

6a. NAME OF PERFORMING ORGANIZATION
U.S. Army War College

6b. OFFICE SYMBOL *(If applicable)*

7a. NAME OF MONITORING ORGANIZATION

6c. ADDRESS *(City, State, and ZIP Code)*
Carlisle Barracks, PA 17013

7b. ADDRESS *(City, State, and ZIP Code)*

8a. NAME OF FUNDING / SPONSORING ORGANIZATION

8b. OFFICE SYMBOL *(If applicable)*

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c. ADDRESS *(City, State, and ZIP Code)*

10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.

11. TITLE *(Include Security Classification)*
ULTRA: A Case Study Unclassified

12. PERSONAL AUTHOR(S)
Mr. Raymond E. Miller

13a. TYPE OF REPORT
Study Project

13b. TIME COVERED
FROM ________ TO ______

14. DATE OF REPORT *(Year, Month, Day)*
91/04/02

15. PAGE COUNT
17

16. SUPPLEMENTARY NOTATION

17. COSATI CODES

FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*

19. ABSTRACT *(Continue on reverse if necessary and identify by block number)*

In 1939, shortly after Britain and France declared war on the Third Reich, the codename ULTRA was conceived by the British MI-6 (and later the United States) to denote sensitive intercept intelligence derived from cryptoanalysis. The British high frequency intercept initiatives focused on Germany's use of the "Enigma" cipher machine, a unit which the Third Reich thought to be totally secure and foolproof from foreign cryptoanalysis attack. The case study is built on several books and articles about the advent of ULTRA and the "Enigma" machine and how sensitive intelligence was collected and disseminated throughout the allied forces during World War II. The books and articles incorporated into this case study are listed in the endnotes and bibliography sections, at the end of the paper.

The purpose of this paper is to provide an insight into the greatest held secret of World War II, the decryption of the German Enigma cipher machine. The decrypted text was classified using the Ultra designator; the contents changed the course of the War, and provided the allies with advanced warnings regarding Hitler's order of battle.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS

21. ABSTRACT SECURITY CLASSIFICATION
Unclassified

22a. NAME OF RESPONSIBLE INDIVIDUAL
DR William Stockton

22b. TELEPHONE *(Include Area Code)*
717-245-3207

22c. OFFICE SYMBOL
AWCAB

Previous editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

USAWC MILITARY STUDIES PROGRAM PAPER

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

ULTRA: A CASE STUDY

AN INDIVIDUAL STUDY PROJECT

by

Mr. Raymond E. Miller
United States State Department

Dr. William Stockton
Project Adviser

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

ABSTRACT

AUTHOR: Raymond E. Miller, U.S. State Department

TITLE: ULTRA: A Case Study

FORMAT: Individual Study Project

DATE: 2 April 1991 PAGES: 17 CLASSIFICATION: Unclass

In 1939, shortly after Britain and France declared war on the Third Reich, the codename ULTRA was conceived by the British MI-6 (and later the United States) to denote sensitive intercept intelligence derived from cryptoanalysis. The British high frequency intercept initiatives focused on Germany's use of the "Enigma" cipher machine; a unit which the Third Reich thought to be totally secure and fullproof from foreign cryptoanalysis attack. The case study is built on several books and articles about the advent of ULTRA and the "Enigma" machine and how sensitive intelligence was collected and disseminated throughout the allied forces during World War II. The books and articles incorporated into this case study are listed in the endnotes and bibliography sections, at the end of the paper.

The purpose of this paper is to provide an insight into the greatest held secret of World War II, the decryption of the German Enigma cipher machine. The decrypted text was classified using the Ultra designator; the contents changed the course of the War, and provided the allies with advanced warnings regarding Hitler's order of battle.

ENIGMA

In October 1919, Dutch inventor Hugo Koch developed and patented a "secret writing machine"; later, he sold the patent to Dr. Arthur Scherbius, a German engineer, who improved Koch's design by incorporating unequal rhythm of movement in the machine's rotors and named it "Enigma"[1]. Dr. Scherbius had hoped to market his cipher machine to the world's business community. He exhibited the machine for the first time at the 1923 Congress of the International Postal Union. In 1924, the German post office used an Enigma to exchange greetings with the Congress; it was publicized in Radio News in America and in a book on cipher machines by the director of the Viennese criminological institute. The machine was originally conceived to protect the secrets of business, but eventually was sold to the armed forces of Germany to protect their secrets. In 1926 the German navy, and in 1928 the army, introduced cipher machines that were modified versions of the civilian model Enigma. In 1930, a military version of Enigma was constructed, whose most essential innovation was a commutator, a "plugboard" with twenty-six plugs and plug connections, that vastly increased the number of possible cipher combinations[2].
In 1933-34, Enigma was adopted by the Germans as a basic, unitary cipher system for the armed forces as well as military intelligence, and other agencies of the Third Reich.

On 1 September 1932, Marian Rejewski, Jerzy Rozycki, and Henryk Zygalski, began work as regular employees at the Polish Cipher Bureau in the general staff building on Warsaw's Saxon square. With Polish-German relations strained due to Germany's tariff and economic war against Poland, the Cipher Bureau concentrated their efforts to break the German codes and ciphers which were being intercepted from radio monitoring.

To facilitate decryption efforts, the Polish Cipher Bureau obtained a commercial type Enigma machine. The machine resembled a typewriter, with an additional panel built into the lid. In the panel were twenty-six little circular glass windows bearing, like the keyboard, the letters of the alphabet; on the panel's underside were a corresponding number of glowlamps. Inside the machine was a set of three rotors, or rotating drums, and a "reversing drum" or "reflector," all mounted on one axle and forming part of an intricate system of wiring. The machine could be powered by a battery or by regular current passed through a small transformer[3]. With every stroke of a key, one or more rotors revolved, i.e., the right hand rotor moves on one position every time a key is pressed. When the right-hand rotor reaches one particular position, known as its "turnover position," the middle rotor also moves ahead one position. Eventually the middle and right-hand rotors may both be in their turnover positions, at which time pressing a letter-key will cause all three rotors to move. The three rotors would have to go through a cycle of 26 x 26 x 26 = 17,576 successive positions before they would return to their starting positions. Each time a key is pressed, encipherment takes place when the rotors have reached their new position[4].

The commercial Enigma solved nothing. It merely provided a general insight into the machine's construction and operation. The cryptologists would have to continue studying the system from the mathematical side, on the basis of the intercepts.

France and Czechoslovakia, like Poland, threatened by German expansion, were natural allies for Poland in collecting intelligence on German armaments and war plans. The first break occurred when the chief of French radio intelligence, Capt. Gustave Bertrand, was approached by a man, introducing himself as an employee of the German Reichswehr cryptographic agency who offered his intelligence services in return for monetary compensation. The German, Hans-Thilo Schmidt, was assigned the code name "Asche" (German for ashes); meetings were arranged on weekends at different locations because Asche could only leave Berlin on the weekends without drawing undue attention to his activities. Over a period of time, Asche provided documents concerning key to manual ciphers used by staff, army signals service, for liaison between military and civil authorities, and with railway police, and others. More importantly, Asche supplied documents on machine ciphers: operating instructions for Enigma; keying instructions, and monthly tables of army keys for December 1931, 1932, 1933, and the first half of 1934[9].

With the above information, Capt Bertrand contacted the Polish Cipher Bureau and arranged a meeting in Warsaw. The Polish were very interested in the material Capt Bertrand had on Enigma; therefore, during the Warsaw meeting in December 1932, a division of tasks was established between Bertrand and his Polish opposite number. The French were to concentrate on furnishing intelligence from Germany that might facilitate the breaking of the machine cipher, the poles on theoretical studies of Enigma intercepts. Procedures were set up for exchange of German radio intercepts, radiogoniometric data, and other intelligence.

The British attack against Enigma took a somewhat different course. In June of 1938, British Intelligence (MI-6) had received a message that would prove to be the most important in the intelligence history of the Second World War. It came from the MI-6 officer at Prague, who reported that he had just returned from Warsaw where, through the Polish intelligence service, he had encountered a Polish Jew who had offered to sell MI-6 his knowledge of Enigma. The Pole had worked as a mathematician and engineer at the factory in Berlin where Enigma was produced. But he had been expelled from Germany because of his religion and had then come to the attention of the British Embassy at Warsaw. The Pole wanted 10,000 British Pounds, a British passport, and a resident's permit for France for himself and his wife. He did not wish to live in England because he had no friends or ties there. The Pole claimed that he knew enough about Enigma to build a replica, and to draw diagrams of the complicated wiring system in each of its rotors. MI-6 decided to send two experts to Warsaw to interview the Pole in person; if satisfied that the information he had was genuine, they were to arrange with MI-6 in Warsaw to take the Pole and his wife to Paris and place him in the charge of the MI-6 resident there. Then, under supervision, the Pole was to re-create the Enigma machine. The Pole passed the tests with flying colors, and was accompanied to France where he began to build the Enigma cipher machine. The end product was about 24 inches square and 18 inches high, and was enclosed in a wooden box. It was connected to two electric typewriters, and to transform a plain-language signal into a cipher text, all the operator had to do was consult the book of keys, select the key for the time of the day, the day of the month, and the month of the quarter, plug in accordingly, and type the signal out on the left-hand typewriter. Electrical impulses entered the complex wiring of each of the rotors of the machine, the message was enciphered and then transmitted to the right-hand typewriter. When the enciphered text reached its destination, an operator set the keys of a similar apparatus according to an advisory contained in the message, typed the enciphered signal out on the left-hand machine, and the right-hand machine printed the plain text[6]. The accuracy of the Pole's machine was later confirmed after the Poles were able to obtain an actual Enigma, which was handed over to an officer of the British cryptographic establishment. Although the Poles and French had penetrated Enigma's ciphers, and the British had managed to create a duplicate of the machine, little could be accomplished unless they had access to the current crypto key which would enable the machine to wcrk. The only way to penetrate the secrets of Enigma was to make another machine that could imitate or interpret the performance of each of the thousands of Enigmas that would come to exist in the German Wehrmacht.

The British foreign office obtained an appropriation in 1938 to build an identical Enigma machine; the contract was let to the British Tabulating Machine Company (BTM) at Letchworth. In complete secrecy, the machine took shape. The final product (named the Bomb), was 8 feet tall and 8 feet wide at its base, shaped like an old-fashioned keyhole. Its secret was in the internal wiring of Enigma's rotors, which the Bomb tried to imitate[7].

MI-6 soon began to input intercepts to the Bomb. The British government had established intercept posts around the world which would record and forward all enemy radio messages to Bletchley Park, where Enigma transmissions were identified, put on tape and fed into the Bomb. The mainstream of German Army intercepts flowed in to Bletchley from a station at Chatham, about thirty miles east of London, near the mouth of the Thames. The Chatham station had a direct teletype link with Bletchley. If the Bomb could find the keys in which the transmissions had been ciphered, the cryptoanalysts at Bletchley could then break the messages.

Six years earlier, the Poles built a duplicate of the Enigma machine. The cryptologists first discovered the function of the reflector, or "reversing drum", then, step by step, reconstructed all the connections in the machine, whose most essential components were a system of rotors revolving about a common axle, and the commutator with its plug connections. Assuming that one could find the crypto keys, the Poles duplicate machine could read the German ciphers. The Poles used an elaboration of methods for reconstructing the Enigma keys exclusively on the basis of the intercepts that were supplied daily by monitoring stations to break the code. Three mathematicians of the Cipher Bureau's German section, Marian Rejewski, Henryk Zygalski, and Jerzy Rozycki, were credited with breaking the code. The main breakthrough came in the final days of December 1932. The practical reading of messages began during the second ten days of January. Just under way in Germany was the Nazi campaign that on 30 January 1933 would deliver power into Hitler's hands. Neither the French nor the British managed to solve the German cipher system.

The experiments at Bletchley were conducted with the utmost secrecy, but with the cryptographers of three nations attempting to read Enigma traffic, the Germans might discover that their secret cipher machine had been compromised. To tighten the security surrounding the Enigma attack, British, French, and Polish intelligence experts held a series of conferences at the Chateau Vignolle, about 25 miles from Paris, where the French cryptographic service worked under the code name "P.C. Bruno.*" The first conference was held on January 9, 1939, whereby the participants decided that since both Poland and France might be overrun in any war with Germany, all vital papers, machines, and personnel connected with Enigma should be concentrated in England. Interestingly, included with the papers from Poland were successful decrypted documents which the Polish General Staff had identified 80 to 90 percent of all the German Wehrmacht units assembled at Poland's borders. At a later conference at a Polish intelligence station in the Pyry forest near Warsaw, the Poles handed over to the British everything in their possession concerning Enigma, retaining only the material that was needed for operational purposes. It was taken under heavy escort to London on July 24, 1939. Only a month later the Germans attacked Poland, and the Second World War began. With the capture of Warsaw and the collapse of the Polish government, the key crptographers involved in Enigma were evacuated from Poland together with the Polish General Staff and the British military mission. The Polish cryptographers were detached by MI-6 and sent to Chateau Vignolle to work with the French.

When the Germans invaded Poland on September 3, 1939, Britain and France finally declared war on Herr Hitler and the Third Reich. Britain was ill-prepared for the conflict, but the Bomb was operational; and it was a machine that promised to provide the most valuable intelligence material of the war -- Ultra.

ULTRA

It was obvious that Ultra would be of use to the British only as long as the Germans remained unaware that Enigma had been penetrated. If they discovered that their secret ciphers were being read by the enemy, they could change to another system which might prove even harder to break. The only way to secure Ultra was to limit its distribution and use among the members of the British high command. To accomplish this task, MI-6 recommended that a new secret agency be established to handle Ultra; its name would be "Special Liaison Units" (SLU's)*. The unit would be staffed by air force officers of proven discretion and MI-6 wireless operators and cipher clerks to handle and route the Ultra intercepts. SLU's would eventually be established at the higher levels of all the British (and later the American) military commands, their particular function being to ensure that no general or admiral, American or British, used Ultra intelligence carelessly, ambitiously, or in such a manner that the enemy might detect that his signals were being read. The task of the SLU's was to convey the substance of solved enemy radio messages to Allied high commands and staffs in Great Britain, the European continent, Africa, Asia, and Australia. The SLU system was one of the best-kept secrets of World War II. According to Wladyslaw Kozaczuk's book "Enigma", the system for ensuring security of information from Enigma decrypts rested on the following principles:

"1. The smallest possible number of persons was to have access to Enigma information;

"2. The list of recipients was to be limited to four or five persons at each of the following main headquarters: supreme headquarters, army groups, principal army and air commands in Europe and Southeast Asia, and British and U.S. air force commands operating from Britain;

"3. The addition of a name to the distribution list required the permission of British intelligence chief General Stewart Menzies' deputy, F.W. Winterbotham;

"4. Commanders, or members of their staffs, cleared for Enigma information were to receive it from their SLU officers personally; the latter were then to destroy the documents;

"5. No Ultra recipient was to transmit or repeat an Ultra signal;

"6. Any action taken by a commander on Ultra information was to be by way of an operations order, command, or instruction that in no way referred to the Ultra signal or could lead the enemy to believe his messages were being read;

"7. Combat operations undertaken on the basis of Enigma information were to disguise the source of the information (for example, reconnaissance aircraft were to be sent out prior to an attack on enemy convoys in the Mediterranean);

"8. No recipient of this information was to voluntarily place himself in a situation that might lead to his capture[10].

In handling Ultra intelligence, is was essential to use the most secure cipher possible in putting Ultra transmissions on the air. Winterbotham insisted that they be in a one-time-pad cipher, the only absolutely secure kind, and that if any government department that received Ultra material wished to put it on the air, this be done through the SLU organization. Ultra would prove the unique experience of knowing not only the precise composition, strength and location of the enemy's forces, but also, with few exceptions, of knowing beforehand exactly what he intended to do in the many operations and battles of World War II.

Ultra's first major intelligence contribution in the Second World War was to warn Britain of "Case Yellow," Hitler's great offensive against western Europe[11]. This information was confirmed when a German courier plane was forced down in Belgium by bad weather and the complete Case Yellow plan fell into Belgian hands. General Bertrand claimed that between October 1939 and the middle of June 1940, the French alone succeeded in obtaining solutions to a total of 141 different Enigma ciphers. Those solutions enabled the French and the British to read about 15,000 German messages.

Hitler issued his first orders for "Operation Sealion"-- the invasion of England--on July 2, 1940[12]. More detailed orders went out on July 16; on August 1, Hitler issued a directive entitled "Conduct of Air and Sea Warfare Against England," with instructions that it was to be put into effect immediately by the Luftwaffe in order "to establish the necessary conditions for the final conquest of England[13]." The Battle of Britain began with massed aerial attacks by the Luftwaffe to bring the RAF Fighter Command to battle and destruction. Goering sought control of the British skies as an essential precondition to invasion by a land army. From the beginning of its campaign, Churchill and the Air Staff were informed, through Ultra, of most, and often all, the Luftwaffe's plans, targets and tactics. This knowledge enabled RAF tacticians to assemble their fighter squadrons at the right place, the right time, and the right altitude, concentrating their main defenses against the primary attacks. After two months of fierce aerial combat, Goering proclaimed September 15 the day when the Luftwaffe would mount a mighty, final onslaught to destroy the RAF. If Eagle Day was successful, Hitler would invade; if it failed, Hitler would not invade. Churchill was fully informed of the Germans' intentions through Ultra. Based on this knowledge the RAF Fighter Command, was able to position their squadrons at the places where they could rise and intercept the German squadrons to the maximum advantage of the RAF. Twenty-five squadrons of RAF Spitfires and Hurricanes engaged the first Luftwaffe fleets, and kept control of the skies over England.

Mr. Alexander S. Cochran, Jr. conducted an interview with Mr. Donald B. Bussey, who was a politics teacher at Princeton University when America entered World War II. Mr. Bussey was recruited into Ultra because he knew one of General George C. Marshall's personal aides and initially worked with the Japanese crypto system Magic in Washington. When asked if the Germans were helpful in the context of their cables, Bussey replied: "They were very methodical; they recorded in great detail at the end of every day for higher headquarters what their complete situation was: order of battle, supply status, maintenance status, operability of tanks and aircraft.[14]" Another question asked of Mr. Bussey was how Ultra intelligence must be integrated with other intelligence. Mr. Bussey responded that "...I personally felt that the most valuable contribution that Ultra made to intelligence operations during the war was in order-of-battle. I was most fortunate here as we could open up this information for wide dissemination very quickly, based upon other sources confirming the same Ultra information.[15]"

Based on countless Ultra intercepts throughout World War II, the allies were in a position to remain one step ahead of the Germans. Ultra was essential to victory in the Battles of Britain and the Atlantic, the war in Africa, and the landings in Sicily and Nor…andy. Without Ultra, victory in the spring of 1945 would have been unthinkable.

In conclusion, it is in the best interests of the United States (and allies) to continue electrical intercept efforts directed against foreign governments. Advanced warning information of the type received by deciphering Enigma traffic during World War II can prove invaluable in directing successful crises operations in the future. As state-of-the-art communications equipment and crypto devices evolve, intelligence collection will become increasingly difficult. Therefore, it is essential that we continue our efforts toward advanced communications technology in order remain one step ahead of adversaries cryptographic efforts throughout the world.

BIBLIOGRAPHY

Brown, Anthony Cave, Bodyguard of Lies. Harper & Row, 1975.

Deutsch, Harold, The Historical Impact of Revealing the Ultra Secret. Parameters VII (No. 3,1977), pp. 16-32.

Deutsch, Harold, The Influence of Ultra on World War II. Parameters VIII (Dec 1978), pp 2-15.

Kozaczuk, Wladyslaw, ENIGMA. University Publications of America, INC, 1984.

Cochran, Alexander S., Protecting the Ultimate Advantage, Military History I (Jun 1985), pp 42-49.

West, Nigel, The SIGINT Secrets. Westintel Research Limited, 1988.

ENDNOTES

[1]. Anthony Cave Brown, Bodyguard of Lies, p. 17.

[2]. Wladyslaw Kozaczuk, ENIGMA, p. introduction xiii.

[3]. Ibid., p. 13.

[4]. Gordon Welchman, The Hut Six Story, p. 45.

[5]. Wladyslaw Kozaczuk, ENIGMA, p. 17.

[6]. Anthony Cave Brown, Bodyguard of Lies, p. 23.

[7]. Ibid., p. 25.

[8]. Wladyslaw Kozaczuk, ENIGMA, p. 82.

[9]. Ibid., p. 100.

[10]. Ibid.

[11]. Anthony Cave Brown, Bodyguard of Lies, p. 36.

[12]. Ibid., p. 40.

[13]. Ibid.

[14]. Military History I (Jun 1985), Protecting the Ultimate Advantage, pp 42-49; Interview with Donald B. Bussey, one of the 28 American Ultra field specialists.

[15]. Ibid.